Exploring Organizational Human Resource Information System Security

Humayun Zafar
Computer Science and Information Systems, Kennesaw State University, Kennesaw, GA, United States., hzafar@kennesaw.edu

Exploring Organizational Human Resource Information System Security

Humayun Zafar, Ph.D.
Kennesaw State University
hzafar@kennesaw.edu

ABSTRACT

We explore HRIS security by presenting information security fundamentals and how they pertain to organizations. With increasing use of enterprise systems such as HRIS, security of such systems is an area that is worthy of concern. Even then, there is surprisingly little research in this area, albeit extensive work is present with regard to HRIS privacy. While focusing on HRIS security we introduce aspects of HRIS security and how it can be enhanced in organizations. Because of its complex, sensitive nature, we suggest that qualitative research is the optimal method of further investigating HRIS security. We also propose six research questions as part of deepening our understanding of HRIS research in the future.

Keywords

Security, HRIS

INTRODUCTION

A Human resource information systems (HRIS) is an integrated computerized system used to acquire, store, manipulate, analyze, retrieve, and distribute pertinent information about an organization's human resources (Tannenbaum 1990). Advances in information technologies have changed the human resource (HR) functions within organizations. Today, most organizations implement an HRIS extensively in support of their basic HR functions, as well as to enhance administrative efficiency, decision making, and information sharing (Lengnick-Hall et al. 2003). In a study conducted by Beadles, Lowery, and Johns (2005), 80% of the HR directors noted that an HRIS improved levels of usefulness of information as well as their ability to disseminate information. Moreover, 90% of the HR directors in their study reported that the HRIS added value to the organization. Accordingly, HR professionals are considered to add value to organizations, since HRIS can free up their time, whereby allowing greater involvement in organizational strategic decisions (Bussler et al. 2002; Hussain et al. 2007).

There is a divergence in HRIS usage. Initially, human resource information systems were developed to replace people with software. Instead of maintaining employee records by HR clerks, data was entered into a system and updated as necessary. Later HRIS was extended to include transaction processing systems (TPS), decision support systems (DSS), communication system, and systems including artificial intelligence (Kovach et al. 2002). As a stand-alone system, usage of HRIS is not only limited to employee record management, but also extended to compensation and benefits, recruitment of talented job applicants and retention (Stone et al. 2005), training and development, managing employee performance (Strohmeier 2007) are additional uses of HRIS. Today, HRIS are no longer stand alone applications but incorporated as a module to enterprise information systems such as Oracle. Thus, HR professionals have access to corporate database and other departments can also have access to the HR department's files. Accordingly, security and privacy are major concerns to ensure only authorized personnel are allowed to have such access (Kovach et al. 2002).

Central to every HRIS is successful implementation, which begins with a comprehensive design (Bedell et al. 2008). The design and implementation of an HRIS can have a significant impact on system effectiveness (Stone et al. 2003). For example, a HRIS may be less engaging than traditional HR systems, and less likely to capture an individual's attention (Stone et al. 2009). It has also been widely acknowledged that poor system design can lead to information security related problems for enterprise wide systems (Baskerville 1993). Organizations should also consider change management, especially in regard to the cultural impact of HR technology on their employees (Bussler et al. 2002). There is extensive research in the area of employee culture and impacts on the information security effectiveness of an organization's technologies (Dhillon 2007).

While there is discussion and research on adoption, implementation, and satisfaction with HRIS, little work has been done on investigating approaches toward maintaining an HRIS while assuring security of the organization and its stakeholders. HRIS security is a pertinent area of concern for organizations. With increased implementation of HRIS as a module of enterprise systems, security is critically important. HR data often include a great deal of confidential data about employees, such as

employment records, payroll and benefits data, social security numbers, test and performance appraisal data, and succession planning, et cetera (DeSanctis 1986; Kovach et al. 1999). As such, companies should be conscientious in managing this type of data.

Keeping in view the paucity of information security related research in HR information systems and information security in general (Zafar et al. 2009), the primary purposes of this study are to discuss (a) information security and its components in general, (b) information security related problems associated with HRIS, (c) guidelines for resolving security and privacy issues, (d) security legislation, and (e) proposed methods of researching effectiveness of HRIS.

WHAT IS INFORMATION SECURITY?

Information security, at times referred to as computer security, is defined as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability (CIA) of information system resources (Stallings et al. 2008). Confidentiality assures that private information is kept safe from unauthorized individuals. It is critical for maintaining the privacy of the employees' personal information (Wong et al. 2009). Integrity assures that information and programs are created and modified in a specified and authorized manner. It is important to assure the integrity of both the data and the system. Availability assures that systems work and service is provided promptly to those who are authorized to use them. Personnel transactions and information processing are increasingly more vulnerable to security threats and risks due to the increased used and complexity of HRIS systems. Accordingly, information security should be a critically important issue of concern for today's HR personnel.

2.1. The Interplay between Security and Privacy

While many consider information privacy as being interchangeable with information security, there are underlying differences between information security and privacy. Kang (1998) clustered privacy into three groupings. The first is concerned with physical space, or protecting an individual's territory from invasion by unwanted objects. In the second view, privacy is primarily concerned with the ability to make a choice without interference. Finally, the third cluster is concerned with the flow of personal information. Specifically, it highlights an individual's control over the acquisition, disclosure, and use of personal information.

There is a litany of research dealing with an array of issues pertaining to HR and HRIS privacy (Alge 2001; Eddy et al. 1999; Stone-Romero et al. 2003; Stone et al. 1998; Stone et al. 2003; Stone et al. 1990). However, as shown in the definition of privacy, the privacy construct deals with an expectation on part of an individual to keep information private. Information security, on the other hand, is concerned with the steps taken to keep the information secure. These steps can vary from technical to managerial controls, and ideally should be viewed synergistically across all organizational boundaries to be implemented successfully. Due to the interplay between information security and privacy, there are several federal and state laws and regulations to safeguard information security and privacy such as the Health Insurance Portability and Accountability Act of 1966 (HIPAA), the Privacy Act of 1974, and Security Breach Notification Law (Wong et al. 2009). A more elaborate discussion of the security legislative process is presented in a later section (Section 5).

SECURITY RELATED PROBLEMS ASSOCIATED WITH HRIS

The primary purpose of an HRIS is to provide accurate and timely information to users of the system. According to Kavanagh & Thite (2009), HR information may be required by various stakeholders, such as HR professionals, managers, and employees. It may be used for strategic decision-making, identifying discrimination problems in hiring to avoid litigation, evaluating effectiveness of training programs, and/or supporting daily operations such as assisting managers monitoring time and attendance of their employees. Kavanagh & Thite further state that this information is gathered from the HRIS database that fits into three categories:

1. Employee biographical information and competencies such as knowledge, and abilities
2. Information about the organization, such as jobs, positions, compensation, and legally required data
3. Data created as a result of the interaction of the first two categories, such as, individual job history, performance appraisals, and compensation information

Due to nature of information stored in an HRIS, it becomes imperative that an organization protects the data. However, confidential information may be disclosed, intentionally, by someone such as a disgruntled employee, or unintentionally, by someone who has not been properly trained in the use of the HRIS. Information can be altered or corrupted, or access to

information by authorized person can be denied. Each of these security threats and/or breaches could negatively impact the organization's result and result in more damaging consequences such as loss of business. law suits, or even bankruptcy (Townsend et al. 2003).

Organizations that use and maintain an HRIS face several major internal and external threats. Following is a discussion of key threats. Internal threats may come from accidental deletion or modification of data due to human errors, intentional damage by disgruntled current or former employees, and employees' unauthorized access to confidential and sensitive data. Human error, although not deliberate, can still result in security breaches. (Werlinger et al. 2009). Examples of human error include forgetting to change passwords, not logging off before leaving a workstation, or careless discarding of sensitive information (Warkentin et al. 2009). This could be due to stress, lack of training or supervision, or bad system design (Lacey 2010). Another type of internal threat is the insider threat. Insider threats are unethical, illegal, intentionally disruptive, and are more dangerous than any type of information security threat (Stanton et al. 2005). A large portion of all convictions for cybercrime involve current or former employees who use their credentials to log into sensitive systems related to organizational components such as HR (Panko 2003). For example, in 2002, a former HR employee at Marsh Incorporated logged into his ex-firm's servers, using login information provided to him while he was still employed (DOJ 2002). Using his privileged access credentials, Washington an employee a $40,000 raise, along with a $100,000 bonus, and destroyed over 900 electronic records. Washington was eventually caught, convicted and sentenced to 18 months in prison. This incident could have been prevented if the former employee's login information would have been deactivated as soon as he was no longer employed at Marsh.

External security threats include viruses, worms, spyware, adware, and Trojans. A computer virus can attach itself to files without the user's knowledge and duplicate itself by executing infected files. When successful, a virus can alter data, erase or damage data, create a nuisance, or inflict other damage (Panko 2003). In a period of five hours in2000, the "I love you" e-mail virus spread infected millions of computers, causing damages estimated at $10 billion (Abreu 2001). Worms such as Code Red, Slammer and MyDoom can spread by themselves without attaching to files (Panko, 2003). Spyware is software installed on an unknowing user's computer that gathers information about the user's activities on the Web (keystrokes, web sites visited, et cetera) and transmits it to third parties such as advertisers or attackers (Stafford et al. 2004). Problems associated with spyware include potential privacy invasion, appropriation of personal information, and interference with the user's computer operation (Stafford et al. 2004).

A Trojan is a type of malicious computer program that usually hides inside email attachments or files and infects a user's computer attachments are opened or programs are executed. Some Trojans can work as spyware, while others can display a login or install screen and collect personal data such as usernames and passwords, or other forms of identification, such as bank account or credit card numbers. They can also copy files, delete files, uninstall applications using remote access programs on the computers, and format disks without alerting the victim.

There are guidelines that can be exercised, whereby reducing and/or avoiding information security related problems. These are presented in the next section.

GUIDELINES FOR RESOLVING HRIS SECURITY ISSUES

Information security personnel recognize that technological measures alone are not sufficient to mitigate threats. Human and organizational measures should be considered as well (Hagen et al. 2008; Werlinger et al. 2009). Accordingly, we suggest a holistic security plan that combines both technological and non-technological measures in creating organizational information security culture. Organizational culture is a system of learned behavior which includes ideas shared or communicated by employees. A strong information security awareness culture is an important factor that leads to success of organizational security (Vroom et al. 2004).

Technological measures

The technological measures related to information security include the technical and physical security mechanisms that prevent, detect, and react to any threats. Examples pertinent to an HRIS include maintaining strong passwords, not sharing user IDs and passwords, and installing anti-virus programs and firewalls. Most software security threats such as malware, viruses, and Trojans could be avoided altogether if all systems were kept current with regard to system patches. However, system patches can actually create additional system vulnerabilities. Therefore, organizations need to test patches and updates in order to ensure that they do not conflict with the HRIS. An application conflict can result in data being permanently damaged (Panko 2003).

Based on our research we have noticed that organizations pay little attention to the very real threats associated with use of enterprise technologies such as Oracle that incorporate HRIS. These systems contain enormous amounts of critical and sensitive information, which is frequently subject to legal, regulatory, and other compliance requirements. In most cases, security and risk professionals, and data owners need to watch for behaviors that may indicate serious HRIS security problems, leading to problems such as the one faced by Marsh Inc. According to Wheatman (2010) some of the roles that may need to be watched are privileged users, legitimate end users, and developers and system analysts. Privileged users have special, high-level privileges to an HRIS, and should be subject to scrutiny from the security professionals. These users have high visibility into, and access to data and any underlying systems. Therefore, they should be subject to background checks and should be monitored and audited for potential problem activities such as addition, modification, or deletion of data, unauthorized addition or removal of employee accounts, and schema modifications.

Legitimate end users have access to an HRIS via some type of application. This, too, presents a security risk for deliberate and/or accidental misuse of that data. Some potential problem behaviors that may need to be monitored in this case are access to data that is not needed for legitimate work, access to data during non-working hours, and access through unapproved channels. We suggest creating user profiles that provide an estimate of the amount of data that users fitting a certain profile may access on a given day. For example, if an employee, on average, accesses 200 Megabytes (MB) worth of data each day, but suddenly starts accessing 900 MB of data, system controls should be in place to notify appropriate personnel of the discrepancy. Although it may be entirely coincidental, situations such as these may uncover potential insider threat issues. Therefore, it is advisable for an organization incorporate thresholds with regard to the amount of data accessed each day. Additional controls should be incorporated regarding the type of HRIS data accessed during non-working hours (e.g., not between 9:00 am and 5:00). Employees should be able to access their personal information during non-working hours. However, should external organizations, such as financial institutions, be able to access HRIS data during non-working hours? Conditions such as these need to be considered. Controls need to be set in place and monitored in these cases.

Accessing an organization's enterprise systems from off-site is a common occurrence via virtual private networks (VPN). The use of VPN has removed the traditional physical network boundary. In that case as well though, access to some systems can still be restricted. For example, a VPN can be used to get access to an organization's electronic mail resources, but not to core systems such as HRIS. Finally, instead of using dedicated applications to HRIS data, employees may knowingly or unknowingly use an application that grants them direct access to an HRIS data table, whereby raising the potential for the raw data to be changed.

Developers and system analysts of an HRIS present two types of risk: potential for data breaches that compromise intellectual property or personal privacy, and more importantly, the ability to change systems that are in live production. Intellectual property and personal privacy can be compromised because developers and systems analysts have the highest levels of privilege and access. These are routinely needed to perform a number of maintenance operations that may be needed to a system. These individuals also have high technical prowess, which grants them the ability to access or change system permissions, as a result granting end users with privileges that they should not have.

Non-technological factors

Developing information security policies is one of the preventative methods to maintain security of an HRIS. Strict adherence to policies assists employees in dealing with processes and procedures to protect information assets and systems. Policies ascertain who is allowed to use a system, an individual's expected behavior during use, and also disciplinary actions for those who violate these policies (Stallings et al. 2008). It is imperative that security policies be established for an HRIS. However, organizational security policies are not effective unless they are communicated to employees and they are closely followed. Therefore, user commitment is needed in order to ensure successful policy implementation. A former study has shown that information security awareness is the most significant indicator in measuring an organization's overall information security performance (Choi et al. 2008).

A security awareness program aims to raise employee understanding of information security guidelines and procedures. It includes education and training as well as awareness-raising initiatives such as emails, pamphlets, and formal presentations. Case studies, scenario planning, and crisis exercises are also used to create awareness, and are an effective means of changing organizational security culture (Hagen et al. 2008; Lacey 2010). According to Johnson (2006), benefits from awareness programs mitigate overall security risks, increase reliability and correctness of information, and result in early detection of potential security incidents.

In the next section, we highlight some of the information security specific legislation that exists.

INFORMATION SECURITY LEGISLATION

As mentioned in the previous section, the widespread use of technology has erased the concept of physical boundaries for businesses. The widespread use of networking technologies such as an HRIS has introduced many windows of opportunity for the naïve person and/or the attacker. This proliferation of technology has resulted in the passage of numerous laws related to technology use and information security. Enterprise software that allows for services such as an HRIS has to abide by the various information security specific regulations that exist. In this section, we provide a brief discussion of the regulations which might impact development and/or use of an HRIS.

Communications Act of 1934 updated 1996

The Communications Act is a wide ranging statue that regulates interstate, foreign and wireless telecommunications (FCC 1996). Certain aspects focus on national security, law enforcement, and intelligence communities. For example, it requires telecommunications providers to establish procedures to require "appropriate authorization to activate interception of communications or access to call-identifying information" and prevent unauthorized interception or access.

Computer Fraud and Abuse Act (1986 – amended 1994, 1996, and 2001)

This act focuses on the threats to digital data and information. It defines and formalizes laws to counter threats from computer related acts and offenses (CFAA 2008). Examples of offenses include accessing, deleting, or distributing computerized information without authorization. This law makes certain activities designed to access a "federal interest computer" illegal. Definition of a federal interest computer is rather broad. Examples include a computer used by a financial institution affiliated with the United States Government, or any computer involved in commission of a crime within the United States.

Computer Security Act of 1987

The Computer Security act provides for improving the security and privacy of sensitive information saved in federal systems (CSA 2008). Sensitive information is defined as any unclassified information that, if lost, or accessed without authorization could potentially impact national interest, or the privacy to which individuals are entitled under the Privacy Act. This act requires federal agencies to identify vulnerable systems, establish training programs to increase security awareness, and establish a plan for the security of each computer system deemed as being vulnerable.

Economic Espionage Act (1996)

The Economic Espionage act pertains to protection of trade secrets (EEA 2007). It was introduced to prevent abuse of information gained by an individual working in one organization while employed by another. Trade secrets refer to all forms and types of financial, business, scientific, technical, economic or engineering information that the owner has taken reasonable measures to protect. Trade secrets may also include information that may not be available to the public.

Electronic Communications Privacy Act of 1986

This act provides insight into the use of cryptography. It is also referred to as the Federal Wiretapping Act (ECPA 2008). It aims to regulate interception and disclosure of electronic information. The law also prevents government entities from requiring disclosure of electronic communications from a provider without proper procedure.

Federal Privacy Act of 1974

The Federal Privacy act is a response to concerns about how extensive use of computerized databases may impact an individual's privacy rights (FPA 2007). It protects an individual's privacy through multiple procedural and substantive rights in personal data. Government agencies must follow fair information practices when acquiring personal data and are restricted with regard to how they can share this data with other people and agencies. Upon request, government agencies are required to inform an individual of any records that they have pertaining to that individual. In addition, this act allows individuals to sue the government for violating any of these provisions.

Gramm-Leach-Bliley Act of 1999 (or Financial Services Modernization Act)

This act enabled the consolidation of commercial banks, investment banks, insurance companies, and securities firms. However, it includes provisions for protecting an individual's personal financial information (GLB 1999). All financial institutions are required to create, implement, and maintain safeguards for the protection of personal information.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA, enacted in 1996, requires establishment of national standards for electronic health care transactions and national identifiers for providers, health plans, and employers (HIPAA 1996). It is assumed that as the industry continues to implement these standards, and increase the use of electronic data interchange, the nation's health care system will become increasingly effective and efficient. This allows for regulation of healthcare, storage, and transmission of sensitive personal information in electronic form.

National Information Infrastructure Protection Act of 1995

This act focuses on criminal intent. It provides federal criminal liability for theft of trade secrets and for "anyone who intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage" (NIIP 1996). It also outlaws the intentional transmission of any program, code, or command that may result in damage to a protected computer, regardless of whether or not access to that computer was authorized. The law also encourages victims to report cyber offenses by permitting them to claim civil remedies for intentional computer crimes.

USA PATRIOT Act of 2001 – H.R. 3162

The official title of this act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001" (PATRIOT 2001). Its main purpose is to deter and punish terrorist acts in the US and around the world. It also enhances law enforcement investigatory tools, and requires financial institutions to report potential money laundering.

As shown, federal laws pertaining to information security have been enacted to ensure that vulnerable systems and, to some extent, individuals are secure. Organizations must focus on the need to establish a consistent set of requirements common to various U.S. and EU jurisdictions, while keeping in mind their own standards for protecting consumer data. However, there may be a gap between organizational understanding and implementation of a law and what the law requires. The privacy requirements of an HRIS are similar to those stipulated by HIPAA. In addition, federal regulations often overlap from one law to another. This overlapping leads to a situation where organizations may not necessarily understand the differences. This could result in non-conformity, and a less secure HRIS system. This problem is further compounded when organizations are required to comply with both U.S. and non-US (e.g. European) regulations. As such, they may need to deal with a patchwork of disparate and over-lapping state and federal regulations, along with privacy rules laid out by individual corporate partners. Within the European Union, organizations are required to deal with the data protection directive, which unlike U.S. regulations such as HIPAA, provides few specifics as to how these privacy requirements should be met.

DIRECTIONS FOR FUTURE RESEARCH

In order to fully comprehend HRIS security, it is important that future research focus on organizational level studies investigating different facets of HRIS security. Since enterprise systems such as the ones that offer HRIS vary in implementations across different companies, a qualitative research method may prove to be a more beneficial choice. Issues such as HRIS adoption, privacy concerns, security, and trust are complex and sensitive in nature, and a qualitative based method will provide the opportunity to provide a rich context to the study. We also contend that this method will also be effective due to the fact that HRIS security and information security in general are naturally intrusive topics. A study can be derailed if participants are initially skeptical about taking part in a study that may highlight information security based problems in their organization (Kotulic et al. 2004). A qualitative research method may assist the researcher in fostering a trusting relationship, which may assist in completion of the research goals. We suggest that HR departments address the following research questions in order to facilitate future research in HRIS security:

1. What are the potential threats to our HRIS, and what has been done to alleviate these threats?
2. What technological security techniques currently enhance our HRIS security?
3. What additional technological security techniques could enhance our HRIS security?
4. What non-technological security techniques currently enhance our HRIS security?
5. What additional non-technological security techniques could enhance our HRIS security?
6. Have we addressed all security and privacy legislation that applies to an HRIS?

CONCLUSION

In this study we explored the under-researched area of HRIS security. We discussed HRIS security related issues, investigated guidelines to cope with these security issues, and also focused on information security specific legislation, and how it can be linked to HRIS security. As a result, we presented six research questions that can be investigated as part of future research. Considering that the use of HRIS and similar enterprise systems will only continue to increase, it is essential that concerns related to HRIS security be addressed.

REFERENCES

1. Abreu, E. (2001) Computer Virus Costs Reach $10.7 Billion This Year, http://www.crn.com/news/channel-programs/18816957/computer-virus-costs-reach-10-7-billion-this-year.htm, Accessed: January 23, 2011.

2. Alge, B. (2001) Effects of computer surveillance on perceptions of privacy and procedural justice, *Journal of Applied Psychology* 86, 4, pp 797-804.

3. Baskerville, R. (1993) Information systems security design methods: implications for information systems development, *ACM Computing Surveys (CSUR)* 25, 4, pp 375-414.

4. Beadles II, N., Lowery, C., and Johns, K. (2005) The Impact of Human Resource Information Systems: An Exploratory Study in the Public Sector, *Communications of the IIMA* 5, 4, pp 39-46.

5. Bedell, M., Canniff, M., and Wyrick, C. (2008) Systems Considerations in the Design of an HRIS, in: *Human Resource Information Systems: Basics, Applications, and Future Directions*, pp. 45-76.

6. Bussler, L., and Davis, E. (2002) Information systems: The quiet revolution in human resource management, *Journal of Computer Information Systems* 42, 2, pp 17-20.

7. CFAA (2008) Computer Fraud and Abuse Act, http://www.justice.gov/criminal/cybercrime/ccmanual/01ccma.pdf, Accessed: January 25, 2011.

8. Choi, N., *et al.* (2008) Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action, *Information Management & Computer Security* 16, 5, pp 484-501.

9. CSA (2008) Computer Security Act of 1987, http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf, Accessed: January 25, 2011.

10. DeSanctis, G. (1986) Human resource information systems: a current assessment, *MIS Quarterly* 10, 1, pp 15-27.

11. Dhillon, G. (2007) *Principles of information systems security: text and cases* Wiley, Hoboken, NJ, p. 450.

12. DOJ (2002) U.S. Sentences Computer Operator for Breaking into Ex-Employer's Database, http://www.cybercrime.gov/leungSent.htm, Accessed: August 23, 2010.

13. ECPA (2008) Electronic Communications Privacy Act of 1986 http://www.it.ojp.gov/default.aspx?area=privacy&page=1285, Accessed: January 26, 2011.

14. Eddy, E., Stone, D., and Stone-Romero, E. (1999) The effects of information management policies on reactions to human resource information systems: An integration of privacy and procedural justice perspectives, *Personnel Psychology* 52, 2, pp 335-358.

15. EEA (2007) The Economic Espionage Act, http://www.justice.gov/criminal/cybercrime/eea.html, Accessed: January 25, 2011.

16. FCC (1996) Communications Act of 1934, http://www.fcc.gov/Reports/1934new.pdf, Accessed: January 25, 2011.

17. FPA (2007) The Privacy Act of 1974, http://www.justice.gov/opcl/privacyact1974.htm, Accessed: January 25, 2011.

18. GLB (1999) Conference Report and Text of Gramm-Leach-Bliley Bill, http://banking.senate.gov/conf/confrpt.htm, Accessed: January 25, 2011.

19. Hagen, J., Albrechtsen, E., and Hovden, J. (2008) Implementation and effectiveness of organizational information security measures, *Information Management & Computer Security* 16, 4, pp 377-397.

20. HIPAA (1996) Health Insurance Portability and Accountability Act of 1996, http://aspe.hhs.gov/admnsimp/pl104191.htm, Accessed: January 26, 2011.

21. Hussain, Z., Wallace, J., and Cornelius, N. (2007) The use and impact of human resource information systems on human resource management professionals, *Information & Management* 44, 1, pp 74-89.

22. Johnson, E. (2006) Security awareness: Switch to a better programme, *Network Security* 2006, 2, pp 15-18.

23. Kavanagh, M., and Thite, M. (2009) *Human Resource Information Systems: Basics, Applications, and Future Directions*, (1 ed.) Sage Publications, Inc, p. 488.

24. Kotulic, A.G., and Clark, J.G. (2004) Why there aren't more information security research studies, *Information & Management* 41, 5, pp 597-607.

25. Kovach, K., and Cathcart, C. (1999) Human Resource Information Systems (HRIS): Providing Business with Rapid Data Access, Information Exchange and Strategic Advantage, *Public Personnel Management* 28, 2, pp 275-282.

26. Kovach, K.*, et al.* (2002) Administrative and strategic advantages of HRIS, *Employment Relations Today* 29, 2, pp 43-48.

27. Lacey, D. (2010) Understanding and transforming organizational security culture, *Information Management & Computer Security* 18, 1, pp 4-13.

28. Lengnick-Hall, M., and Moritz, S. (2003) The impact of e-HR on the human resource management function, *Journal of Labor Research* 24, 3, pp 365-379.

29. NIIP (1996) National Information Infrastructure Protection Act of 1995, http://www.justice.gov/criminal/cybercrime/s982.htm, Accessed: January 26, 2011.

30. Panko, R. (2003) *Corporate Computer and Network Security* Prentice-Hall, Inc., Upper Saddle River, NJ.

31. PATRIOT (2001) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf, Accessed: January 24, 2011.

32. Stafford, T., and Urbaczewski, A. (2004) Spyware: The ghost in the machine, *Communications of the Association for Information Systems* 14, pp 291-306.

33. Stallings, W., and Brown, L. (2008) *Computer Security: Principles and Practice* Pearson Prentice Hall, Upper Saddle River, NJ.

34. Stanton, J.*, et al.* (2005) Analysis of end user security behaviors, *Computers & Security* 24, 2, pp 124-133.

35. Stone-Romero, E., Stone, D., and Hyatt, D. (2003) Personnel selection procedures and invasion of privacy, *Journal of Social Issues* 59, 2, pp 343-368.

36. Stone, D., and Lukaszewski, K. (2009) An expanded model of the factors affecting the acceptance and effectiveness of electronic human resource management systems, *Human Resource Management Review* 19, 2, pp 134-143.

37. Stone, D., Lukaszewski, K., and Isenhour, L. (2005) E-Recruiting: Online strategies for attracting talent, in: *The Brave New World of eHR: Human Resources Management in the Digital Age,* H.G. Gueutal and D. Stone (eds.), Jossey-Bass, San Francisco, CA, pp. 22-53.

38. Stone, D., and Stone-Romero, E. (1998) A multiple stakeholder model of privacy in organizations, in: *Managerial ethics: Moral management of people and processes,* M. Schminke (ed.), Erlbaum, Mahwah, NJ, pp. 35–59.

39. Stone, D., Stone-Romero, E., and Lukaszewski, K. (2003) The functional and dysfunctional consequences of human resource information technology for organizations and their employees, in: *The functional and dysfunctional consequences of human resource information technology for organizations and their employees,* D. Stone (ed.), JAI Press., Greenwich, CT, pp. 37-68.

40. Stone, E., and Stone, D. (1990) Privacy in organizations: Theoretical issues, research findings, and protection mechanisms, *Research in Personnel and Human Resources Management* 8, 3, pp 349-411.

41. Strohmeier, S. (2007) Research in e-HRM: Review and implications, *Human Resource Management Review* 17, 1, pp 19-37.

42. Tannenbaum, S. (1990) Human resource information systems: User group implications, *Journal of Systems management* 41, 1, pp 27-32.

43. Townsend, A., and Bennett, J. (2003) Privacy, technology, and conflict: emerging issues and action in workplace privacy, *Journal of Labor Research* 24, 2, pp 195-205.

44. Vroom, C., and Von Solms, R. (2004) Towards information security behavioural compliance, *Computers & Security* 23, 3, pp 191-198.

45. Warkentin, M., and Willison, R. (2009) Behavioral and policy issues in information systems security: the insider threat, *European Journal of Information Systems* 18, 2, pp 101-105.

46. Werlinger, R., Hawkey, K., and Beznosov, K. (2009) An integrated view of human, organizational, and technological challenges of IT security management, *Information Management & Computer Security* 17, 1, pp 4-19.

47. Wheatman, J. (2010) Ten Database Activities Enterprises Need to Monitor, http://www.gartner.com/DisplayDocument?id=1361013, Accessed: December 9, 2010.

48. Wong, Y., and Thite, M. (2009) Information Security and Privacy in HRIS, in: *Human Resource Information Systems: Basics, Applications, and Future Directions,* M. Kavanagh and T. Mohan (eds.), Sage Publications.

49. Zafar, H., and Clark, J.G. (2009) Current State of Information Security Research in IS, *Communications of the Association for Information Systems* 24, Article 34, pp 557-596.